

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
31 October 2002 (31.10.2002)

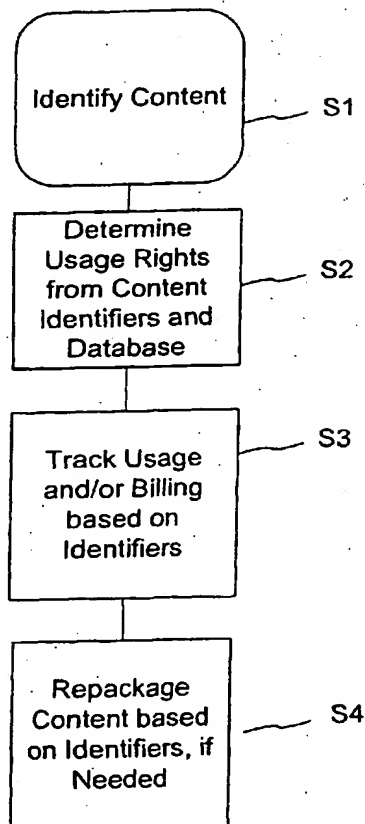
PCT

(10) International Publication Number
WO 02/086803 A1

- (51) International Patent Classification⁷: **G06K 9/00**,
G06F 17/30
- (21) International Application Number: **PCT/US02/12171**
- (22) International Filing Date: **19 April 2002 (19.04.2002)**
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (30) Priority Data:
60/285,514 20 April 2001 (20.04.2001) **US**
60/315,569 28 August 2001 (28.08.2001) **US**
10/126,921 18 April 2002 (18.04.2002) **US**
- (71) Applicant (for all designated States except US): **DIGI-MARC CORPORATION** [US/US]; 19801 SW 72nd Avenue, Suite 100, Tualatin, OR 97062 (US).
- (72) Inventors; and
(75) Inventors/Applicants (for US only): **LEVY, Kenneth, L.** [US/US]; 110 NE Cedar Street, Stevenson, WA 98648 (US). **RHOADS, Geoffrey, B.** [US/US]; 2961 SW Turner Road, West Linn, OR 97068 (US). **HIATT, R., Stephen** [US/US]; 3210 SW Gale Avenue, Portland, OR 97201 (US).
- (74) Agent: **STEWART, Steven, W.**; Digimarc Corporation, 19801 SW 72nd Avenue, Suite 100, Tualatin, OR 97062 (US).
- (81) Designated States (national): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.**

[Continued on next page]

(54) Title: **USER-FRIENDLY RIGHTS MANAGEMENT SYSTEM AND METHODS**



(57) Abstract: A method of performing digital asset management of content is provided. The content is identified (S1) with an identifier. The usage rules can be maintained on a remote or local database or server. Once extracted, an identifier is used to index the database to locate a corresponding usage rule (S2), and can be used to override copy control information with proper purchase and subsequent protection. In another embodiment, an identifier is used to track usage (S3), such as amount of content viewed, time played, and copies made.

WO 02/086803 A1



(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— with international search report

USER-FRIENDLY RIGHTS MANAGEMENT SYSTEM AND METHODS

Related Application Data

[0001] The present application claims the benefit of U.S. Patent Application No. _____, titled "User-Friendly Rights Management System and Methods," filed April 18, 2002 (Attorney Docket No. P0617) and U.S. Provisional Application Nos. 60/285,514, filed April 20, 2001 and 60/315,569, filed August 28, 2001.

Technical Field

[0002] The present invention relates to integrating identified content with digital rights management systems. The present invention also relates to multimedia signal processing, such as steganographically encoding auxiliary information into media signals, and decoding the auxiliary information from the media signals.

Background and Summary Of the Invention

[0003] As digital content continues to proliferate, management of digital assets becomes an increasingly difficult challenge. The term "content" is broadly defined herein and may include audio, video, images, electronic data, biometric information, graphics and designs, electronic documents, copyrighted materials, software, multimedia content, etc., etc. Sometimes we interchangeably use the term "media" instead of content in this document. Enhancements in computer networking and database technology allow companies to manage large content collections and to make the content available to third parties. While network communication provides a powerful tool to enable a database manager to share content with others, it makes it more difficult to control and track how the content is being used.

[0004] For example, some companies maintain extensive content databases to promote their products. Customers or service providers such as advertising and

- 2 -

marketing firms can access this content remotely via an internet, extranet, web site, intranet, LAN, WAN, wireless network or file transfer transactions. Although computer networking telecommunication technology facilitates access, it makes it difficult to ensure that customers and services providers are getting the latest content, and that they are getting accurate and helpful information relating to the content.

[0005] There is a need to enable digital rights management systems to reliably link content with additional, related data -- including related content. The terms "link" and "linking" are defined broadly herein to include associating, pointing to, facilitating the access of, linking, connecting or connecting to, revealing an storage address of, and/or facilitating database interrogation, etc. There is also a need for a digital rights management system to reliably link content with related usage billing information. One way to associate content with information about the content is to place the information in a file header or footer. This approach is not terribly attractive because the added information often does not survive file format changes, conversion to the analog domain, and is susceptible to being stripped away, etc. We believe that an improved approach to associate content with related data is to steganographically hide identifying information within the content. One example of steganography is digital watermarking.

[0006] Digital watermarking is the science of encoding physical and electronic objects with plural-bit digital data, in such a manner that the data is essentially hidden from human perception, yet can be recovered by computer analysis. Most commonly, digital watermarking is applied to media such as images, audio signals, and video signals. However, it may also be applied to other types of data, including documents (e.g., through line, word or character shifting), software, multi-dimensional graphics models, and surface textures of objects. In physical objects, the data may be encoded in the form of surface texturing, or printing. Such marking can be detected from optical scan data, e.g., from a scanner, optical reader, input device, digital camera, or web cam. In electronic media (e.g., digital audio or imagery -- including video), the data may be encoded as slight variations in sample values. Or if the media is represented in a so-called orthogonal domain (also termed "non-perceptual," e.g., MPEG, DCT, wavelet,

- 3 -

etc.), the data may be encoded as slight variations in quantization values or levels. The assignee's U.S. Patent Nos. 5,862,260 and 6,122,403, and U.S. Application No. 09/503,881, filed February 14, 2000, are illustrative of certain digital watermarking technologies. A great many other approaches are familiar to those skilled in the art. The artisan is presumed to be familiar with the full range of literature about steganography, data hiding and digital watermarking.

[0007] Digital watermarking systems typically have two primary components: an encoder that embeds the watermark in a host media signal, and a decoder that detects and reads the embedded watermark from a signal suspected of containing a watermark (e.g., a suspect signal). The encoder embeds a watermark by altering the host media signal. For example, the encoder (or embedder) component embeds a watermark by altering data samples of the media content in the spatial, temporal or some other transform domain (e.g., Fourier, Discrete Cosine, Wavelet Transform domains). The decoder component analyzes a suspect signal to detect whether a watermark is present. In applications where the watermark encodes information, the decoder extracts this information from the detected watermark.

[0008] The analysis of the detected data can be accomplished in various known ways. Presently, most steganographic decoding relies on general-purpose microprocessors that are programmed by suitable software instructions to perform the necessary analysis. Other arrangements, such as using dedicated hardware, reprogrammable gate arrays, or other techniques, can of course be used.

[0009] According to one aspect of our invention, a digital watermarking system includes (or communicates with) a secondary component -- a database. Such a database preferably includes data related to content. The related data may include, e.g., content owner or copyright information, metadata, usage rights, enhanced or interactive content, and billing information, etc. This related data is preferably organized or linked according to respective content identifiers. For example, if the content includes a song and the related data includes usage rules, then the usage rules can be associated with the song via a content identifier that is unique to the song or to a class of related songs.

- 4 -

The database can be stored locally, remotely, or both. The database can also be distributed, with different databases stored in different networks or locations, such as a complete central and mirrored database and local databases including only subsets of the related data on a local computer. Of course our usage of the term database throughout this document is broad enough to include software-based databases, data structures, data records, etc., etc.

[0010] User-friendly digital rights management systems are preferred in our evolving digital and connected world. Many digital rights management systems fail because they focus solely on the content owner's security desires and not on consumer usage. As such, these rights management systems are not acceptable to consumers. A historical example is taken from the software industry in the 1980's, when that industry abandoned copy protection. We have solved some of the failing associated with traditional digital rights management systems. Our inventive user-friendly digital rights management system provides transparent usage models to consumers while protecting the content. In one implementation, a user-friendly rights management system enables consumers to easily purchase content that they want to play or use, as opposed to stopping consumers from using the content. One benefit of our inventive system is that it is now easier for a mass market to purchase content, rather than use illegitimately obtained content.

[0011] In one embodiment of the present invention, a digital watermark embedded within a content item is used to convey a content identifier(s). In a second embodiment, file headers associated with a content item include a content identifier(s). In still another embodiment, both digital watermarks and file headers are used to carry content identifiers. Content identifiers can be linked to related data, such as "usage rights" (or "usage rules") common in some digital rights management (DRM) systems. (The artisan is presumed familiar with the many DRM systems, a few of which are described in U.S. Patent Nos. 5,765,152, 5,410,598, 5,943,422, 6,363,488 and 6,330,670. Of course there are many other DRM systems and containers that can be enhanced by the present invention.). These rules typically define the scope of permissible content use, e.g., such as regulating printing, viewing, copying, altering,

- 5 -

distributing, selling, etc. Digital watermarks -- including a content identifier -- can be used for content tracking and data management. In another embodiment, digital watermarks are used in connection with DRM content containers. Another aspect of the invention is a method of performing digital asset management of media content. In even another embodiment the copy protection state (also known as copy control information including copy freely, copy no more, copy never, and/or copy once) can be overridden through linking the identifier to usage rules, if the usage rules allow copy protection information to be overridden, e.g., to enable the sale or distribution of the content. This enables the content owners to be properly paid, and users to share content, instead of merely prohibiting use of the content.

[0012] One aspect of the present invention provides content owners with copy protection security and royalty tracking, and end-users with an easy-to-use system that improves current content distribution methods, such as CD, DVD and VHS. A combination of watermarking and DRM techniques can be employed, where a watermark allows content to leave and be found outside an associated DRM package without harming the security of the system. The watermark identification can link the content to the usage rules, and, optionally, the usage rules can dictate whether the content should be re-packaged into the DRM package if found outside of it. This means that content found outside the DRM package can be purchased and used, as well as re-secured, as opposed to that content being considered illegal and perhaps destroyed. This inventive feature increases the revenue generated from the content. A DRM package is broadly defined and may include an encryption-based format, or a container in which content is securely maintained, etc. Artisans know many DRM packaging techniques, which may be suitably interchanged with the packaging aspect of the present invention. DRM systems help publishers or content owners prevent unauthorized copying, replication, usage or distribution of their software products, either via CD-ROM, via the Internet, transfer, etc. Other DRM systems incorporate encryption, digital signature and license manager technologies, and enable authentication from either a disc, online database, or from a PC hard drive. These technologies can be applied to secure CD-ROM or computer executable files, and to maintain desired control over the distribution of content during its life cycle. A DRM

- 6 -

package that allows licensing and reporting provides an ideal rights management system for audio, video and images.

[0013] Still another aspect of the present invention is to provide an efficient distribution chain based on identified content, particularly when combined with our inventive techniques. Yet another aspect of the present invention is linking together databases that are stored and protected by a network of the database owner, and enabling those databases to function as one database via a central router and database.

[0014] Further features, advantages and benefits will become apparent with reference to the following detailed description and drawings.

Brief Description of the Drawings

[0015] Fig. 1 illustrates a flow diagram of a content management process according to one embodiment of the present invention.

[0016] Fig. 2 illustrates a system for enhancing digital content management by identifying content, and linking the content with usage rules or permissions.

[0017] Fig. 3 illustrates an inventive content distribution chain.

[0018] Fig. 4 illustrates a content identifier format.

[0019] Fig. 5 illustrates a database structure for the distribution chain illustrated in Fig. 3.

[0020] Fig. 6 illustrates an intelligent content distribution system, including linking databases via a central router to enhance efficiency and privacy of metadata.

[0021] Fig. 7 illustrates a content distribution chain including a reporting system and a billing system.

[0022] Fig. 8 illustrates the structure of Fig. 5, including billing information.

[0023] Fig. 9 demonstrates a distributed database exemplar system.

Detailed Description

Rights Management System

[0024] With reference to Fig. 1, a rights management system preferably includes four steps. In step S1, content, whether within an encryption package or not, is identified before rendering. ("Rendering" here has its familiar meaning of presenting for visual and/or audible inspection, e.g., on a TV, audio player, etc. Our use of the term "rendering" is broad enough to include transferring, copying and distributing.). Content is preferably identified by steganographically encoding data within the content, such as in the form of a digital watermark. The digital watermark preferably includes a unique content identifier. Content can be alternatively identified via frame and/or segment headers.

[0025] Usage rights are determined in step S2 via linking the content identifier to external data (e.g., data defining the usage rules). In general, usage rules define the scope of permitted use for respective content. Examples of usage rules include the scope of permissible copying, rendering, transferring, altering, playing, viewing, printing, distributing, using, etc. Content identifiers can be used to organize a database that is maintained locally or remotely (e.g., a central usage system). Once extracted from content, an identifier can be then used to interrogate the database to retrieve the usage rules. Content usage is regulated based on its corresponding usage rules.

[0026] Content usage can be tracked via an identifier in step S3. This usage tracking can be used, e.g., for proper billing to the consumer and payment to content owners and providers. Tracking can be incremental or per content item. In one embodiment, each video frame or every nth frame (or audio segment) is uniquely or redundantly

- 8 -

identified. Tracking identifiers per frame (or audio segment) allows for a "pay-as-you-go" system, in that a consumer can be billed for only the amount of content they view, access or listen to. In another embodiment, billing is based on a one-time access fee.

[0027] As a fourth and optional step (step S4), if content is found outside of its respective DRM, and it should be in the DRM package as dictated by related usage rules, the content identifier can help facilitate repackaging of the content in a DRM container. Initially, the identifier will help identify the content. The identifier can also identify or point to a specific package or packaging protocol, or the identifier can link to repackaging requirements. If desired, an identifier can be used to help put content back into an encryption package. An identifier can also be linked to usage rules, which can regulate content usage, even for content outside of a package. Examples of content being located outside of a container include transferring the content to a different medium, or converting from a digital format to an analog format. Since the content identifier is content specific, e.g., it is associated with the content and not the container, it persists with the content, even when the content is found outside of a container.

[0028] The preceding second through fourth steps preferably proceed on the assumption that the content has been packaged in an encryption container (or other DRM format) and digitally watermarked (or otherwise identified) prior or during distribution. Content that is not protected nor identified can be handled under default system rules, such as allowing unrestricted usage or view-only usage.

[0029] In a preferred implementation, the identifier is provided via a digital watermark, potentially combined with header data for additional access. An advantage of a digital watermark identifier is that the watermark will typically survive end-user recording of the content onto new media or into a new format. This new format may be desirable for end-users to use multiple rendering devices, or used to try to bypass the security system. However, identifying the content itself helps to enforce security features and continue to track content, even when the content is found outside of a DRM container.

- 9 -

[0030] Optionally, the embedded data (e.g., a digital watermark) can provide fine-grain usage and quality of content monitoring as well as copy protection. An example of fine grain usage is to monitor content subsets, such as an audio segment or set of video frames. A watermark can be redundantly embedded per frame or segment, or different watermarks can be embedded per each frame or segment, to allow counting or monitoring of the content subsets.

Home Network System

[0031] A home rights management system 10 is shown in Fig. 2. System 10 includes a local home network (indicated by the dashed-line box labeled "Home"). The local home network includes a home content server 30 in continuous or intermittent communication with rendering devices 40-42. The operation of our inventive system 10 is preferably indifferent to how content stored on the home content server 30 is initially obtained, and indifferent to whether the content is packaged in an encryption or other DRM package. The system 10 architecture and system 10 operations are described below.

[0032] Home content server 30 can include a personal computer that has downloaded compressed content from a web site or peer-to-peer site via the internet. Alternatively, home content server 30 can be a set-top box (STB) with suitable computing functionality. Or home content server 30 can include a storage device with computing, database and communication functionality. Of course, home content server 30 need not be located in a home, but may be located in an office, building, garage, theater, mobile computer, handheld device, etc.

[0033] Returning to Fig. 2, system 10 preferably includes a central database 20 and a central billing agency 50. Central database 20 and central billing agency 50 can be associated or otherwise communicate (e.g., as shown by the dashed-line box labeled "Internet . . ." in Fig. 2). Of course the invention is not so limited. Indeed, there need not be interaction between database 20 and agency 50. In addition, agency 50 may be contacted only monthly, when, e.g., the home content server 30 reports its monthly

- 10 -

usage. Central database 20 can communicate with home center server 30, via a network such as the internet (e.g., via a cable modem, modem or DSL), dial-up network, dedicated network, LAN, WAN, etc. Central database 20 is preferably contacted whenever new content, which was not sent with its usage rules to be stored in a local database such as home content server 30, enters the home network. In another embodiment, central database 20 includes a plurality of distributed databases, which are synchronized or which include specific subsets of content (e.g., based on region, genre, content, etc.). In another embodiment, central database 20 includes a plurality of peer-to-peer nodes. Database management software can be used to help track and manage content, content identifiers, and related content.

[0034] Central database 20 preferably maintains a set of usage rules. The usage rules define use limits for related content. The usage rules can be communicated to various network locations, such as to home content server 30. Home content server 30 can query central database 20 to obtain or update usage rules, or updated rules can be pushed to home content server 30. Server 30 can also cache the usage rules locally, or can occasionally query database 20 to obtain updates, etc.

[0035] Preferably, each of rendering device PC 40, STB/TV (or VCR, PVR or DVD, etc.) 41 and portable player 42 communicates with home content server 30, either continuously or intermittently. In one embodiment, some or all of the rendering devices communicate over a wireless channel. Of course, the invention is not so limited. Indeed, the rendering devices can communicate through other channels as well (e.g., via USB, parallel ports, communication links, IEEE 1394, firewires, modems, coaxial cable, twisted pair, etc., etc.). In some implementations server 30 streams content to the rendering devices for real time play. In other implementations server 30 downloads the entire content or subset of the content to the devices. Some rendering devices may be able to decrypt the content (if the content is encrypted or other DRM protected) and detect a content identifier, e.g., an embedded digital watermark. Other rendering devices may rely on the home content server 30 for decryption (if needed) and identifier detection.

- 11 -

[0036] When content playing is requested, a rendering device 40-42 or home content server 30 checks the content item and/or frame headers for an identifier. In one embodiment, checking for an identifier includes a watermark detection process. In another embodiment, checking the content item includes extracting data from a file header. In still another embodiment, checking for an identifier involves both checking header data and detecting an embedded watermark.

[0037] In the case of checking a file header, if an identifier is found, and it is not part of an authenticated encryption package, it is self-authenticated. (This is particularly so when dealing with digital signatures or encryption authentication, etc.). This self-authentication process helps to ensure that the identifier has not been modified, including that it has not been copied from other content.

[0038] If a header identifier is not available or trusted, the content can be searched for a watermark identifier. (Alternatively, in another embodiment, an initial search for a watermark identifier is made.). Watermarks are inherently trusted due to the secrecy of their embedding key and/or self-authentication features. In an alternative embodiment, a so-called fragile watermark is used to enhance the security of an identifier. A fragile watermark can be designed to be lost, or to degrade predictably, when the data set into which it is embedded is processed in some manner. Thus, for example, a fragile watermark may be designed so that if an image is JPEG compressed and then decompressed, the watermark is lost. Or if an image is printed, and subsequently scanned back into digital form, the watermark is corrupted in a foreseeable way. Similarly, if a video or audio signal is converted from digital to analog the fragile watermark is corrupted or altered. (Fragile watermark technology is disclosed, e.g., in commonly assigned applications 09/234,780, 09/433,104, 09/498,223, 60/198,138, 09/562,516, 09/567,405, 09/625,577, 09/645,779, and 60/232,163.). By such arrangements it is possible to infer how a data set has been processed by the attributes of a fragile watermark embedded in the original data set.

[0039] If the content is not identified, the home content server 30 (or rendering device) can handle the content according to a default usage rule or otherwise in a

- 12 -

predetermined manner. For example, the server may allow unrestricted usage, or may permit a onetime play with copy restrictions. Alternatively, the home content server 30 may query central database 20 to receive guidance.

[0040] Once the content is identified, however, and the central database 20 provides usage rules associated with the content identifier, the home content server 30 or rendering device 40-42 determines whether, and/or to what extent, the content can be rendered according to the usage rules. The rendering device 40-42 may enforce these rules, or the home content server 30 may enforce them by withholding content from a rendering device 40-42 and 45 that it is not authorized to render the content. Since content is identified by content identifiers (e.g., digital watermark data), content can be tracked, managed, and rendered, even if it has left an encryption package. Indeed, linking an identifier to usage rules helps to ensure that the content can be controlled, even with out an encryption package.

[0041] In another embodiment, embedded data (e.g., watermark data) is extracted and used to determine if the content is even allowed outside an encryption package, and cause any open format content to be encrypted before it is played.

[0042] The identifier can also allow usage (e.g., playing, recoding, transferring, etc.) of the content to be tracked. In one embodiment, the tracking monitors each time that a content item is accessed. In another embodiment, the tracking determines how much of the content item is actually played. For example, if an identifier is continuously embedded throughout the content, either as metadata in frames or as digital watermarks, the identifier can be used to track how much of the content is played (e.g., a digital watermark counter). Further discussion regarding these and other techniques are found in assignee's copending U.S. Patent Application No. 09/574,668, filed May 18, 2000. Otherwise, frame-counting (or group of frames-counting) techniques can monitor the amount of content usage.

[0043] System 10 can optionally save watermark "bookmarks," so users can begin playing where they left off. In this case, a watermark identifier can be used to uniquely

- 13 -

identify a location, chapter or segment within the content item. An identifier can then be used to index back into the content, much like a conventional bookmark.

[0044] A watermark identifier can also be even used to track quality by checking for degradation of the embedded data, such as through bit errors.

[0045] The home content server 30 can use tracking information (e.g., amount of content played, which content is accessed, types of use, etc.) to interact with a central billing agency 50. Central billing agency 50 can communicate with home content server 30 via the internet or other communications channel.

[0046] Central billing agency 50 can help facilitate billing for content consumed and/or used. Central billing agency 50 can also help ensure that other system participants, including content owners and providers, are properly paid. Optionally, the billing agency can provide information to the consumer about current billing and pricing on content before playing the content.

[0047] If content is not allowed to be played on the local home system or its usage rights are not known, the home content server 30 can obtain rights from central database 20. This process can be facilitated via internet or other communications channel. Alternatively, central or local information linked to an identifier can be used to provide the end-user directions on how to obtain rights. Thus, if content is obtained elsewhere, possibly from a file-sharing network or directly from a friend, the usage rights can be easily obtained from identifier-provided information. (Additional disclosure regarding using embedded data with file sharing can be found in assignee's U.S. Patent Application No. 09/620,019, filed July 20, 2000.).

[0048] While the content is being played, the content identifier can be optionally used to provide or link to other information via additional data and links maintained in a content server or central database 20. This information can include new releases by the same artist or director, similar movies or songs, and related merchandise, etc. (U.S. Patent Application Nos. 09/620,019 and 09/571,422, filed May 15, 2000, include

- 14 -

disclosure regarding linking to other information and actions via embedded data.). In addition, this information may provide opportunities to purchase the described or related items. Additionally, the identifiers can be used to link to interactive content, such as found on a web site.

[0049] A watermark identifier can provide additional advantages, such as providing copy protection bits within the embedded data that can be used to restrict or prohibit distribution (e.g., copying, transferring, rendering, etc.) of content to a format or media that may allow illegal distribution, such as a recordable DVD or CD. For example, home content server 30 may prohibit transfer of content, based on the copy protection bits, to recording device 45. If copy protection bits require that the content cannot be copied, but a content identifier links to usage rights or to a copy permission (either of which indicates permission for re-using or copying the content), the subsequently obtained permission preferably overrides the copy protection bits. In this case, a billing or central router can communicate to the home content server a permission (or updated usage rule) to indicate that the content can be re-used or copied according to permission. Hence, the permission or updated usage rule trumps the copy protection bits. (Of course obtaining the permission can be conditioned on payment or other billing requirements.). For non-DVD video and non-DVD or SDMI audio content, the presence of a specific watermark protocol can identify the content as protected. A fragile watermark can also be added for copy-once (i.e. one generation) capabilities, if desirable. In another embodiment, the presence of the watermark is determined in hardware, without reading the payload bits, thus reducing the cost of the copy control hardware. Then, the watermark payload is decoded in software. (Further discussion regarding copy control bits can be found in assignee's U.S. Patent Application No. 09/620,019.).

[0050] Thus, our rights management system is transparent and easy-to-use for the end-user, and allows copyright owners to protect and robustly track their content.

Distribution Chain

[0051] Traditionally, content is sent in a distribution chain from a content owner to a distributor, and then on to a service provider (e.g., a VOD service provider) that may include either (or both) of a cable/satellite operator and online retailer. The content is then provided to a client (e.g., a home consumer). Our distribution chain, e.g., such as a video on demand (VOD) chain, is now described with respect to Fig. 3.

[0052] The content is preferably uniquely identified. Content can be identified, e.g., by a digital watermark. In some cases the digital watermark includes a unique ID. The unique ID preferably includes at least a content identifier, and may also include a content owner ID, distributor ID, VOD service provider ID and/or a Retailer ID, as shown in Fig. 4. Of course alternative or additional fields can be used for a unique ID.

[0053] The unique ID and usage rules (e.g., for each of the distributor, operator, retailer, and consumer) are preferably created by the content owner and entered into an ID system. In one embodiment, an owner creates a unique ID by querying an ID system (or database) to obtain a unique identifier. These usage rules (or "rights") regulate the permissible use by the various distribution chain participants. The usage rules are indexed via the unique ID. The ID system preferably includes a database to help manage the content owner's unique IDs and usage rules and to help ensure that any given ID is not redundantly assigned. Preferably, the unique ID can be read at various participant points in the Fig. 3 distribution chain. The unique ID can be used to determine the usage rules at these various participant points. For example, the Distributor can access the unique ID and query the ID system to retrieve distributor-related usage rules. The ID System may optionally include an authenticated method to identify the participant (e.g., distributor, service provided, consumer). There are many suitable authenticating methods known in the art, e.g., such as providing a user ID, account number, IP address, digital signatures, numeric identifiers, etc. Of course other authenticating methods may be suitably interchanged with this authentication aspect of the present invention. The ID system determines the proper usage rules for a requesting participant and then returns the usage rules to them. The ID system can also

- 16 -

return other desired information or links (e.g., URL, IP address, e-mail list, etc.). For example, the ID system may return a link to access information regarding the actors in a subject movie and their new releases. Or the link may relate to a particular audio file or song that is being played by the consumer. If a proprietary player or plug-in to the player is provided by the last member of the chain before the consumer, such as the retailer, the retailer ID does not need to be embedded and can be obtained from the proprietary player. However, if this content is found unpackaged outside the authorized consumer environment, it is advantageous to have the retailer ID as part of the digital watermark unique ID so the retailer's rules can be applied and the retailer is properly paid for that content.

[0054] The ID system can include a master database or a plurality of databases. (Of course the ID system will typically include a computer or server, running database management software, to help manage the database.). Our preferred database format, shown in Fig. 5, is used when a unique ID includes the ID of the requesting participant (e.g., Distributor ID, retailer ID, etc.) and its related usage rules. With this format, the unique ID identifies the requesting participant. So during a database interrogation no additional information, besides the Unique ID, needs to be communicated to the database. The participant verification can be enhanced by using authenticated IDs including encryption and digital signatures, as well as different watermark algorithms (or payload structures) for each participant, where only that participant knows the algorithm. The secret part of the algorithm may vary a pseudo-random (PN) sequence for each participant. This process is also known as secret key watermarking.

[0055] The ID system may be maintained on one or many distributed central servers, as well as being "intelligently" distributed, as shown in Fig. 6. Intelligent distribution includes storing various unique IDs and usage rules (and optionally related content, e.g., URLs, IP addresses, etc.) on local databases within each participant site of the distribution chain shown in Fig. 3 (e.g., in the Distributor Database or the Retailer Database, etc.). Preferably, the locally stored data is relevant only to the local participant. For example, the VOD Operator Database preferably includes only those usage rules that are relevant to the VOD operator. Or the Consumer database includes

- 17 -

only those usage rules and related content that are relative to the subject video (or audio) content.

[0056] A content owner creates (for his/her content) unique IDs and usage rules (and optionally related content) for each of the distribution chain participants. In one implementation, a content owner creates a unique ID by query central router database to obtain a suitable ID. Of course many content owners (A-C) may create unique IDs and usage rules as shown in Fig. 6. A central router and database are used to route the usage rules and any related data to a correct distribution chain participant. The central router database preferably only includes content owner IDs and content owner database addresses. In addition, the unique ID and database content is pushed from a content owner database to each other participant, including the consumer for content that she has licensed, through the central router. The database content can include the original content (videos, audio, etc.), usage rules and any related content (e.g., URLs, IP addresses, web pages, etc.). The pushed database content preferably includes only that information which is relevant to a particular participant. The distributor, VOD operator, retailer and consumer databases preferably only include the usage rules for that distributor, VOD operator, retailer and consumer, respectively. Local databases (e.g., the consumer and distributor databases) can be automatically updated such as hourly, daily, weekly, etc., to remain fresh and up-to-date information. No one database or router needs to include all the content's usage rules, which helps to ensure security for the content. Participants also benefit since they rarely need to request usage rules from the central server because the usage rules for their content are regularly pushed to them. The usage rules can be periodically updated. In the example structure shown in Fig. 5, the database entries which include that participant's ID and related information are stored in that participant's network and database.

Billing System

[0057] The Fig. 4 unique ID can be used to maintain usage reporting and royalty billing, as shown in Fig. 7. Fig. 7 shows a centralized Reporting System and a centralized Billing System. Of course these systems can include computers and/or

- 18 -

servers, tracking and accounting software executing on the servers and computers, and communications hardware/software, etc. The various participants (e.g., distributor, service provider, consumer, etc.) can be accurately billed for their access and/or handling of content based and tracked according to the unique ID. Of course the various participants can establish accounts with the billing system, to facilitate billing, automatic billing, etc. (In the case of a permission overriding copy protection bits, described above, a consumer can establish an account so that when she requests permission to distribute copy-protected content, the account is automatically billed when the permission to distribute is sent to the consumer.). Usage is preferably reported to the reporting system according to the unique identifiers. Of course, the Reporting Systems and Billing Systems shown in Fig. 7 can be distributed so that each participant keeps track of their own billing similar to the Fig. 6 distributed system.

[0058] Some of the above-mentioned databases are described as including usage rights. These databases can be expanded to include billing information, as shown in Fig. 8. When the modified data structures are accessed, usage information can be optionally stored in the consumer's home system and updated to central systems to help track usage reporting and royalty billing, as shown in Fig. 7. The billing and reporting systems do not usually need to receive updates as often as the content usage rules. For example, the billing and reporting systems may be updated from the home system every two weeks or every month or so.

Example

[0059] A distribution chain including a content owner A, VOD operator B, consumer C, and a video D is presented by way of example to illustrate one aspect of the present invention. Related, intelligently distributed databases are shown in Fig. 9, where the central router database is located in mirrored locations for the central router, the content owner A database is located in mirrored locations within the content owner A's network, and the VOD operator B database is located in mirrored locations within the VOD operator B's network.

- 19 -

[0060] For this example we assume that video D includes a digital watermark embedded therein. The digital watermark preferably includes a unique ID that at least uniquely identifies the video as video D. When consumer C wants to watch video D, the consumer's player (or plug-in to the player, or central home server, etc.) decodes the digital watermark to extract the unique ID. The extracted unique ID is communicated to the central database. The central database uses the unique ID to identify a VOD operator B identifier, which is used to locate the VOD operator B's database (or database IP address). The unique ID is also used to locate an owner A identifier (ID), which is used to locate a content owner A's database (or database IP address). (We note that an alternative implementation involves communicating a unique ID, like the one shown in Fig. 4, which also includes the content owner ID and VOD provider ID. The central database uses the content owner ID and VOD ID to find the appropriate owner and VOD database IP address.). Once found, the content owner A's database provides usage rights for consumer C's usage, and the VOD operator B's database provides the consumer's pricing. Then, consumer C is informed of their rights for viewing and the price of, oh say \$4.00 per view, by the player. The consumer can signal acceptance via the player, or viewing the video D can be deemed acceptance of the terms.

[0061] For example, lets now suppose that the consumer C watches the video D one and a half times. The amount of viewing is locally tracked in the player by counting or detecting digital watermarks that are embedded in video frames throughout the video D, e.g., embedded to correspond with 1 second intervals. The player reports the usage (along with the unique ID) to the central router database (or alternatively to the VOD operator B database). The amount owed for this usage, \$6.00, can be recorded in the VOD operator billing information. (Of course, we expected that traditional billing methods, e.g., pre-authorization of a credit card or monthly billing, etc., can be used to collect or manage the amount due and can be stored locally until updated, such as to the VOD operator's billing system.). Based upon the unique ID, usage amount, and billing information provided to the content owner A via the VOD operator B, the content owner A is paid its share of the amount owned, e.g., perhaps 50% of the \$6.00 (or \$3.00).

[0062] Alternatively, a third party or clearinghouse is used for billing and reporting. In this case the player can report the unique ID and usage amount to the third party. Of course it would be beneficial to allow the content owner A access to the third party reporting to understand the amount and type of their content that is used.

Concluding Remarks

[0063] Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms.

[0064] The various section headings in this document are provided for the reader's convenience and provide no substantive limitations. Of course, the subject matter under one section can be readily combined with the subject matter under another section.

[0065] The methods, processes, and systems described above may be implemented in hardware, software or a combination of hardware and software. For example, the watermark data encoding processes may be implemented in a programmable computer or a special purpose digital circuit. Similarly, watermark data decoding may be implemented in software, firmware, hardware, or combinations of software, firmware and hardware. The methods and processes described above may be implemented in programs executed from a system's memory (a computer readable medium, such as an electronic, optical or magnetic storage device). Finally, a content owner and content ID can be combined into one content ID which is desirable in situations, such as for audio and video content, where content owners, such as record labels and movie studios, are sold and traded between content groups.

[0066] The particular combinations of elements and features in the above-detailed embodiments are exemplary only.

- 21 -

We claim:

1. A method of performing, on a consumer device, rights management of media content comprising:
identifying the media content with a steganographic identifier;
packaging the identified media content in an encrypted package; and
linking the media content to usage rules via the steganographic identifier.
2. The method according to claim 1, wherein said identifying step comprises digitally watermarking the media content to include an identifier.
3. The method according to claim 1, wherein said identifying step comprises digitally watermarking the media content to include an identifier comprising a content identifier and at least one of a distributor identifier, a retailer identifier and an owner identifier.
4. The method according to claim 1, wherein the usage rules comprises at least one of the following rules: copy control, usage limitations, rendering criteria, and playback restrictions.
5. The method according to claim 2, wherein the identifier includes copy protection bits.
6. The method according to claim 1 further comprising the step of tracking the media content based on the identifier.
7. The method according to claim 6, further comprising the step of incrementally tracking the media content.

- 22 -

8. The method according to claim 2, further comprising the steps of digitally watermarking a plurality of location identifiers in the media content, each location identifier identifying a location in the media content, and indexing into the media content with at least one of the location identifiers.
9. The method according to claim 2, further comprising the steps of identifying the media content via the identifier when the content is found outside of the package, and accessing the usage rules with the media content identifier to determine whether the media content should be repackaged in at least one of an encryption package and digital rights management container.
10. The method according to claim 2, further comprising the step of restricting distribution of the media content based on usage rules accessed by the identifiers.
11. A system for rights management comprising:
a personal computer including:
a memory; and
electronic processing circuitry in communication with said memory via a communications bus,
wherein said memory includes computer executable software instructions stored therein for execution on said electronic processing circuitry, the software instructions including instructions to: i) handle content including a content identifier steganographically embedded within the content; ii) decode the steganographically embedded content identifier from the content; iii) enable use of the content according to usage rules, the usage rules being associated with the content identifier; and iv) track the use of the content.
12. The system according to claim 11, further comprising at least one rendering device in communication with said computer, wherein the use comprises rendering of the content via the rendering device.

- 23 -

13. The system according to claim 12, further comprising at least one database in communication with said computer, wherein the database includes the usage rules, and wherein the computer executable software instructions further comprise instructions to communicate the content identifier from the computer to the database, wherein the database is interrogated with the identifier to obtain the usage rules associated with the content, and wherein said computer executable software instructions further comprise instructions to receive the usage rules when communicated to the computer from the database.

14. The system according to claim 13, wherein said enabling instructions restricts usage for the content based on the usage rules.

15. The system according to claim 14, wherein the steganographic embedding comprises digital watermarking.

16. The system according to claim 12, wherein a digital watermark component comprises the identifier.

17. The system according to claim 16, wherein said computer executable software instructions further comprise instructions to track usage of the content based on the content identifier.

18. The system according to claim 17, wherein the identifier comprises a plurality of identifiers, each corresponding to a location in the content.

19. The system according to claim 17, wherein said system further comprises a billing agency in communication with said computer, and wherein tracked content usage is communicated to the billing agency, and wherein the usage rules dictate whether content owners are to be paid for usage via the billing agency rather than blocking usage of the content.

- 24 -

20. A method to regulate a content distribution chain including a plurality of participants, said method comprising the steps of:

providing a unique identifier for a content item, the content item to be handled in the content distribution chain;

associating a plurality of usage rule sets with the unique identifier, wherein each of the plurality of sets corresponds to at least one of the plurality of participants; and

regulating the content item for a participant according to its respective usage rule set.

21. The method according to claim 20, wherein said unique identifier is embedded in the content item via digital watermarking.

22. The method according to claim 21, wherein the usage rule sets define the scope of permissive use of the content item, and wherein the scope of permissive use includes at least one of copying, viewing, rendering, distributing, reformatting, packing, transferring and printing.

23. The method according to claim 22, wherein the plurality of participants include at least one of a distributor, service provider and consumer.

24. The method according to claim 23, wherein the identifier comprises a content identification and at least one of an owner identification, a distributor identification and a retailer identification.

25. The method according to claim 22, wherein the content item comprises at least one of video or audio, and the usage rule set mandates that payment for the usage is to be made rather than blocking usage of the content.

26. A method of regulating distribution of digitally watermarked content comprising the steps of:

decoding a digital watermark in the digitally watermarked content, the digital watermark comprising at least one component related to copy usage;

- 25 -

obtaining the copy usage component from the decoded digital watermark; and prohibiting the distribution of the digitally watermarked content according to the copy usage component unless a permission to distribute the content is received, and then a decision of whether to prohibit distribution of the digitally watermarked content is determined based on the permission instead of on the copy usage component.

27. The method of claim 26, wherein the digital watermark further comprises at least one component related to content identification, wherein said method further comprises the steps of:

communicating the content identification component to a database, the database using the content identification component to identify at least one of: i) billing information related to distribution of the content, and ii) the permission; and receiving the permission from the database.

28. The method of claim 27, wherein the permission is associated with a billing or payment for distribution of the content.

29. The method of claim 27, wherein the distribution comprises at least one of copying, transferring and rendering.

30. The method of claim 26, wherein the digital watermark further comprises a content identification component and the content identification component comprises the content usage component.

31. A distribution system to handle content including at least one identifier steganographically embedded therein, said system comprising:

a plurality of databases, wherein each of the plurality of databases is associated with a system participant;

a central router to communicate with each of the plurality of databases; and

at least one content database to communicate with the central router, wherein the content database communicates a unique set of usage rules associated with the content identifier to each of the plurality of databases via the central router, the unique

- 26 -

sets of usage rules being determined at least in part on usage requirements for each of the databases.

32. A method to regulate content in a distribution chain, the content including an identifier, the method comprising the steps of:

for at least a first participant and a second participant in the distribution chain, storing a first set of usage rules and a second set of usage rules, respectively, at each of a first participant site and a second participant site; and

at each of the first participant site and second participant site, respectively regulating use of the content in accordance with the first set of usage rules and second set of usage rules.

33. The method according to claim 32, wherein the sets of usage rules defines the permissive scope of use for the content.

34. The method according to claim 33, further comprising the step of associating the content to a set of usage rules via the identifier.

35. The method according to claim 34, wherein the identifier comprises a digital watermark component.

36. The method according to claim 35, further comprising the step of communicating an updated set of usage rules to at least the first participant site.

37. The method according to claim 36, wherein the updated set of usage rules is communicated through a central router.

38. The method according to claim 37, further comprising the step of reporting from the first participant site to the central router information corresponding to the usage of the content.

- 27 -

39. The method according to claim 38, further comprising the step of using the reported information to facilitate billing.

40. A method of repackaging content into an encryption container or digital rights management (DRM) container when the content is found outside of a container, the content comprising a digital watermark embedded therein, the digital watermark including a content identifier, said method comprising the steps of:

decoding the digital watermark from the content to obtain the content identifier, the content identifier identifying the content;

providing the content identifier to a database, the database including usage rules associated with the content identifier, the usage rules comprising at least one rule regarding repackaging;

based on the repackaging rule, determining whether the content should be repackaged in at least one of an encryption container and DRM container; and, if indicated by the determination,

packaging the identified content in at least one of an encryption container and DRM container.

41. A method comprising the steps of:

analyzing a content item to determine whether a digital watermark is steganographically embedded therein; and if the digital watermark is detected in the content,

abiding by a usage rule including at least one of an instruction to encrypt and an encryption protocol; and

encrypting the content item according to the usage rule.

42. The method of claim 41 wherein the usage rule is predetermined and a decision to encrypt the content item is dependent on both of the usage rule and an output channel through which the content item will be communicated.

43. The method of claim 42, wherein the output channel comprises a consumer device capable of copying or distributing the content item.

- 28 -

44. The method of claim 43, wherein the device comprises at least one of a compact disc player and digital video disc recorder.

45. The method of claim 41, wherein the instruction to encrypt is dependent on an output channel through which the content item will be communicated.

46. The method of claim 45, wherein the output channel comprises a consumer device capable of copying or distributing the content item.

47. A method comprising the steps of:
analyzing a file header associated with a content item to determine whether the header includes an indicator; and if the indicator is detected in the header,
abiding by a usage rule including at least one of an instruction to encrypt and an encryption protocol; and
encrypting the content item according to the usage rule.

48. The method of claim 47 wherein a decision to encrypt the content item is dependent on the usage rule and dependent on an output channel through which the content item will be communicated.

49. The method of claim 48, wherein the output channel comprises a consumer device capable of copying or distributing the content item.

50. The method of claim 47, wherein the instruction to encrypt is dependent on an output channel through which the content item will be communicated.

51. The method of claim 50, wherein the output channel comprises a consumer device capable of copying or distributing the content item.

52. A system for managing a content item comprising:
a system memory; and

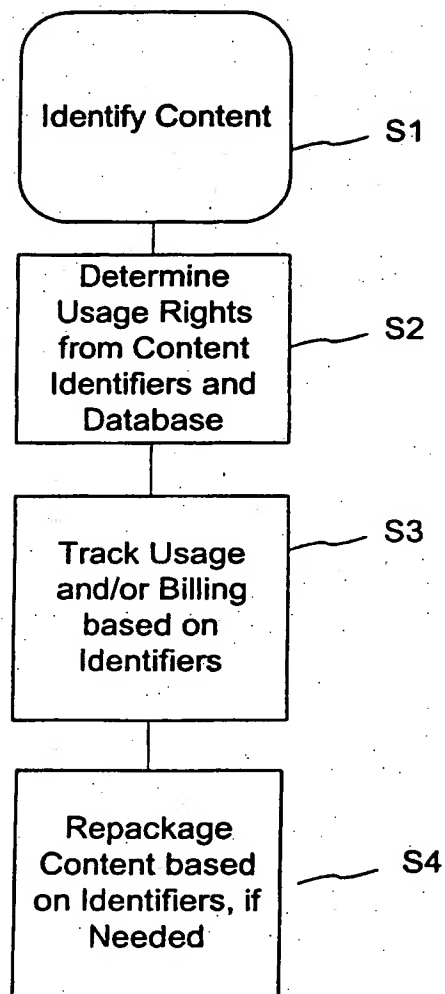
- 29 -

electronic processing circuitry in communication with said memory via a communications bus,

wherein said memory includes computer executable software instructions stored therein for execution on said electronic processing circuitry, the software instructions including instructions to: i) determine whether the content item includes a steganographic identifier embedded therein; and if the content does not include the steganographic identifier, ii) abide by a default usage rule including at least one of an instruction to encrypt and an encryption protocol; and iii) encrypt the content item according to the usage rule.

53. The system of claim 52 wherein the steganographic identifier is embedded in the content item in the form of a digital watermark.

FIG. 1



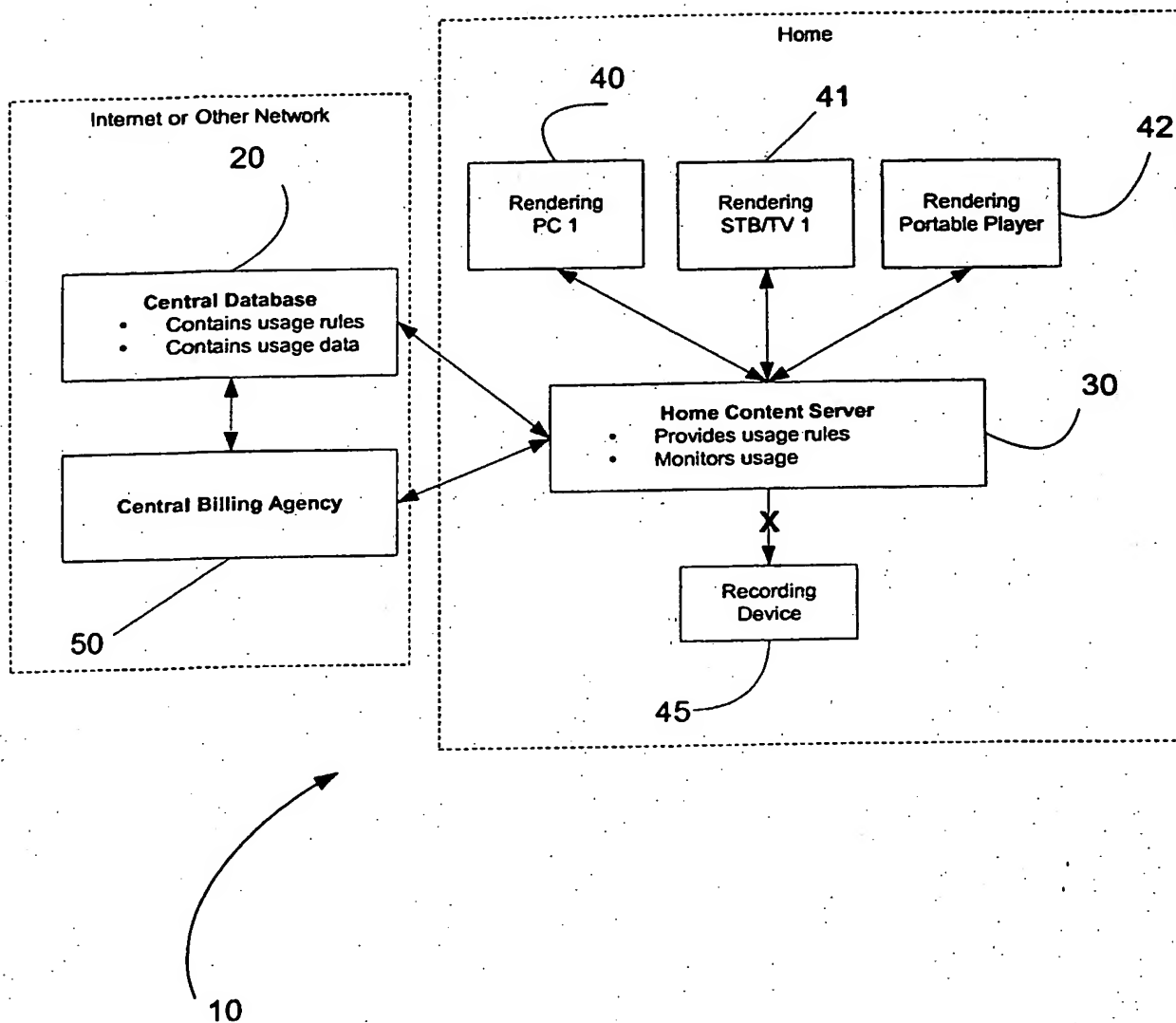


FIG. 2

3/5

Fig. 3

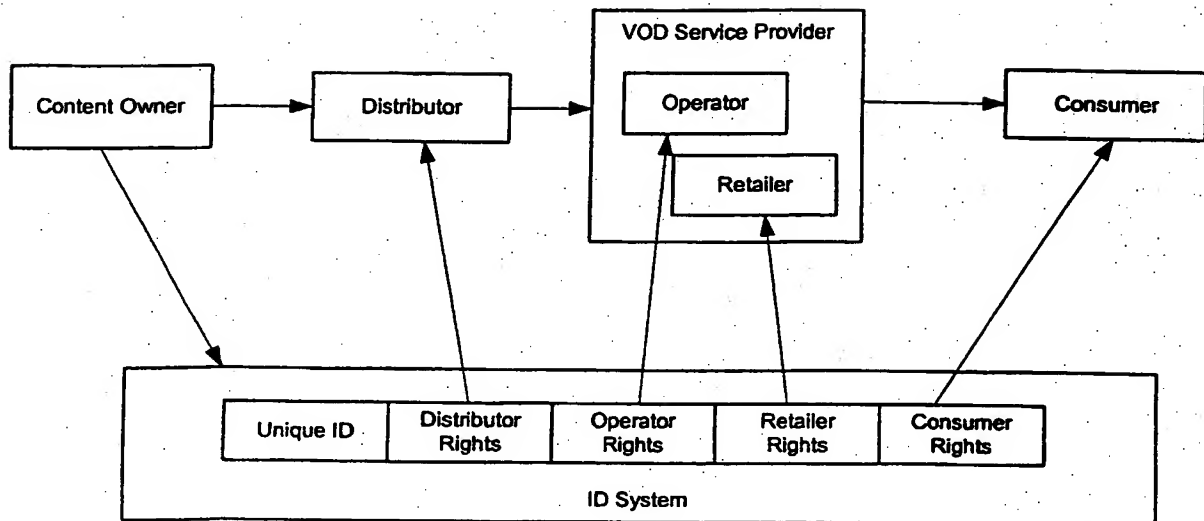


Fig. 4

Unique ID				
Content Owner ID	Content ID	Distributor ID	VOD Operator ID	Retailer ID

Fig. 5

Unique ID			Usage Rules
Content Owner ID	Content ID	Distributor ID	Distributor Usage Rules
Content Owner ID	Content ID	VOD Operator ID	VOD Operator Usage Rules
Content Owner ID	Content ID	Retailer ID	Retailer Usage Rules
Content Owner ID	Content ID	N/A	Consumer Usage Rules

4/5

Fig. 6

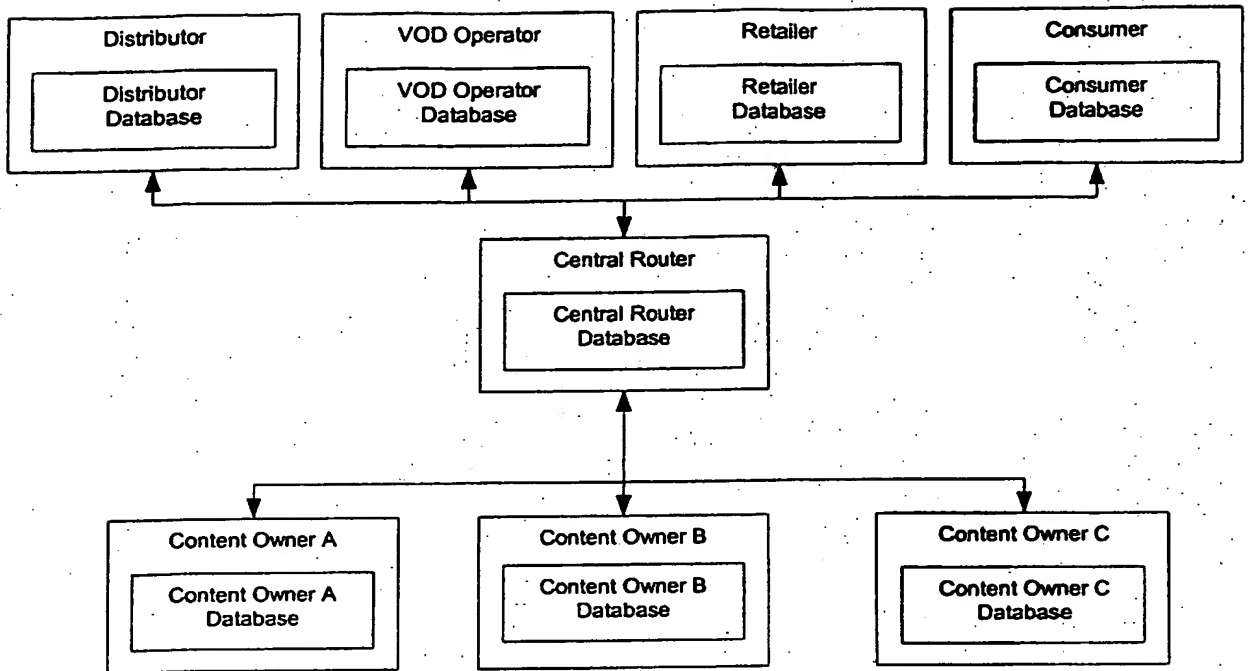


FIG. 7

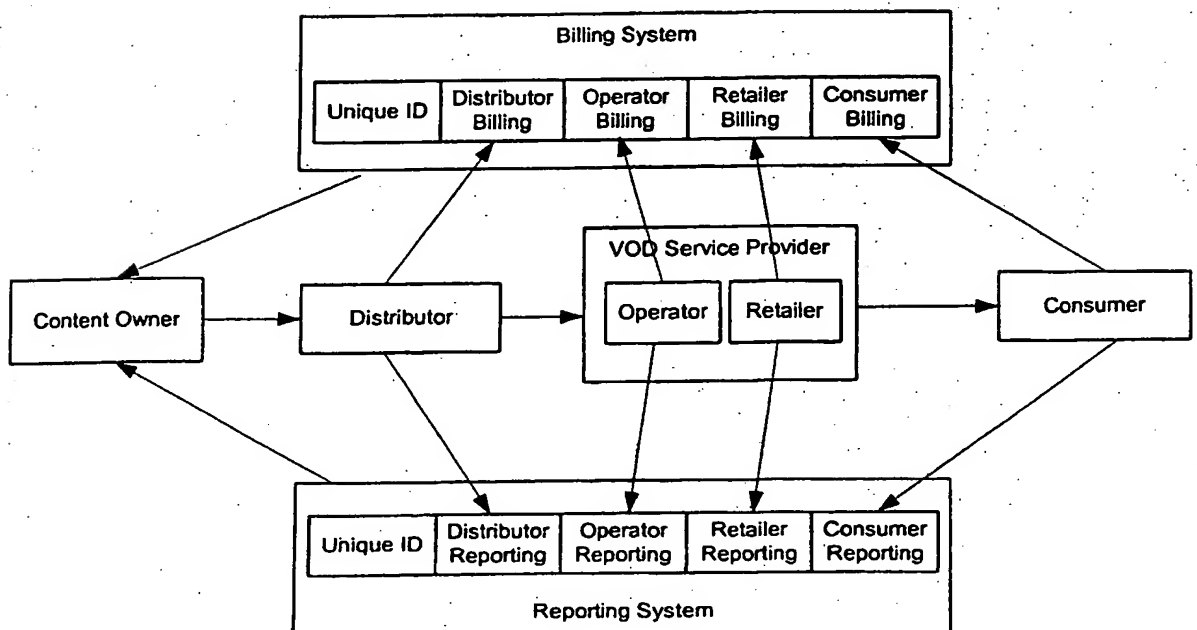


Fig. 8

Unique ID			Usage Rules	Billing Information
Content Owner ID	Content ID	Distributor ID	Distributor Usage Rules	Price to VOD Operator
Content Owner ID	Content ID	VOD Operator ID	VOD Operator Usage Rules	Price to Retailer
Content Owner ID	Content ID	Retailer ID	Retailer Usage Rules	Price to Consumer
Content Owner ID	Content ID	N/A	Consumer Usage Rules	Price to Distributor

Fig. 9

BEST AVAILABLE COPY

Central Router Database	
Content Owner A ID	Content Owner A IP address
VOD Operator B ID	VOD Operator B IP Address

Content Owner A Database				
Unique ID			Usage Rules	Billing Information
Content Owner ID	Video D ID	VOD Operator ID	VOD Operator Usage Rules	Price to Consumer
Content Owner ID	Video D ID	N/A	Consumer Usage Rules	Price to VOD Operator

VOD Operator B Database			
Unique ID		Usage Rules	Billing Information
Content Owner ID	Video D ID	VOD Operator Usage Rules	Price to Consumer

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/12171

A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : G06K 9/00; G06F 17/30 US CL : 382/232; 707/10 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 382/232; 707/10 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	U S 5,956,716 A (KENNER et al) 21 September 1999, the whole document	1-53
Y	U S 5,850,481 A (RHOADS) 15 December 1998, the whole document	1-53
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "B" earlier application or patent published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "A" document member of the same patent family		
Date of the actual completion of the international search 06 June 2002 (06.06.2002)		Date of mailing of the international search report 09 SEP 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230		Authorized officer Leo Boudreau Telephone No. (703) 305-4750 <i>Rugenia Zogan</i>

Form PCT/ISA/210 (second sheet) (July 1998)

THIS PAGE BLANK (USPTO)